Lesson 1 - Information Systems Security and IA

Introduction
What is IA?
Foundation for IA
The Future
Goals of IA
Your Role in Security
Summary

Topics

Introduction

Information Assurance (IA) awareness training is not only a matter of common sense, but is mandated by the government.

In this lesson, we are going to look at what IA is and the laws that necessitate this training.

Learning Objectives

After you have completed this lesson you will be able to:

- Identify the laws associated with IA awareness training
- Define IA
- Identify the goals of IA

Lesson 1 - Information Systems Security and IA

Introduction
What is IA?
Foundation for IA
The Future
Goals of IA
Your Role in Security
Summary

Topics

What is IA?

IA is considered to be many different things by different people.

Information Operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Lesson 1 - Information Systems Security and IA

Introduction
What's IA?
Foundation for IA
The Future
Goals of IA
Your Role in Security
Summary
Topics

Foundation for IA

Below are two of the many laws that initiated IA training. (Click on the manuals located in the graphic to learn more about **OPNAVINST 5239 & Public Law 100-235** and the **Computer Security Act of 1987**.)

Lesson 1 - Information Systems Security and IA

Introduction
What's IA?
Foundation for IA
The Future
Goals of IA
Your Role in Security
Summary

Foundation for IA

Below are two of the many laws that initiated IA training. (Click on the manuals located in the graphic to learn more about **OPNAVINST 5239 & Public Law 100-235** and the **Computer Security Act of 1987**.)

OPNAVINST order 5239 is the order that requires you to receive Information Assurance Awareness training.

Back

Lesson 1 - Information Systems Security and IA

Introduction
What's IA?
Foundation for IA
The Future
Goals of IA
Your Role in Security
Summary
Topics

Foundation for IA

Below are two of the many laws that initiated IA training. (Click on the manuals located in the graphic to learn more about **OPNAVINST 5239 & Public Law 100-235** and the **Computer Security Act of 1987**.)

The Computer Security Act of 1987 mandates that Federal Agencies implement security guidelines and standards, and provide periodic training to everyone involved with Federal computer systems containing sensitive, unclassified information.

Lesson 1 - Information Systems Security and IA

Introduction
What is IA?
Foundations for IA
The Future
Goals of IA
Your Role in Security
Summary
Topics

The Future

In the future we will see more "cyber warfare". Spies may try to use the computer to:

- **Monitor activities**
- **Access information**
- **Sabotage data**
- **Disrupt communications**
- **Pass bad information**

If you and all other government end users make IA an everyday procedure, it will become second nature and allow you to protect your work and information from these threats.

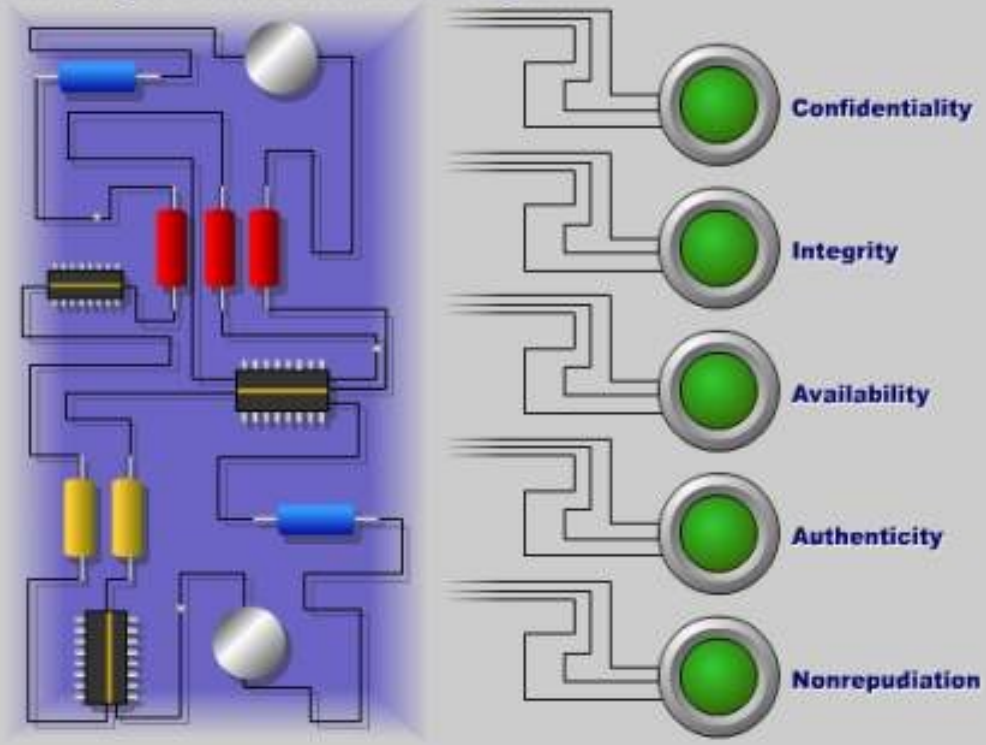
Lesson 1 - Information Systems Security and IA

Introduction
What's IA?
Foundation for IA
The Future
Goals of IA
Your Role in Security
Summary
Topics

Goals of IA

Glossary Term: Nonrepudiation

The five goals of IA are confidentiality, integrity, availability, authenticity, and nonrepudiation. Click on the green buttons to learn about these goals.



Lesson 1 - Information Systems Security and IA

Introduction
What's IA?
Foundation for IA
The Future
Goals of IA
Your Role in Security
Summary
Topics

Goals of IA

Glossary Term: Nonrepudiation

The five goals of IA are confidentiality, integrity, availability, authenticity, and nonrepudiation. Click on the green buttons to learn about these goals.

CONFIDENTIALITY AVAILABILITY INTEGRITY AUTHENTICITY NONREPUDIATION

Confidentiality

Only the people who have the rights to the information are passing it.

You, as an end user, will need to make sure that only the people who need to have the information are the ones getting the information.

Lesson 1 - Information Systems Security and IA

Introduction
What's IA?
Foundation for IA
The Future
Goals of IA
Your Role in Security
Summary
Topics

Goals of IA

Glossary Term: Nonrepudiation

The five goals of IA are confidentiality, integrity, availability, authenticity, and nonrepudiation. Click on the green buttons to learn about these goals.

Integrity

CONFIDENTIALITY AVAILABILITY
INTEGRITY AUTHENTICITY
NONREPUDIATION

The information being passed is accurate.

You can easily imagine what might happen if the location of enemy troops was entered into a computer inaccurately for a bombing mission. The wrong place would be bombed, you might have an event involving friendly fire on your own troops, or innocent civilians might be injured or killed - all because of inaccurate or corrupted information.

Lesson 1 - Information Systems Security and IA

Introduction
What's IA?
Foundation for IA
The Future
Goals of IA
Your Role in Security
Summary

Topics

Goals of IA

Glossary Term: Nonrepudiation

The five goals of IA are confidentiality, integrity, availability, authenticity, and nonrepudiation. Click on the green buttons to learn about these goals.

CONFIDENTIALITY **AVAILABILITY**
INTEGRITY AUTHENTICITY
NONREPUDIATION

Availability

The information can be accessed.

Do the appropriate people have access to the information?

Think about what could happen if you don't turn in your timesheet to your boss in time to get paid.

Lesson 1 - Information Systems Security and IA

Introduction
What's IA?
Foundation for IA
The Future
Goals of IA
Your Role in Security
Summary
Topics

Goals of IA

Glossary Term: Nonrepudiation

The five goals of IA are confidentiality, integrity, availability, authenticity, and nonrepudiation. Click on the green buttons to learn about these goals.

Authenticity

CONFIDENTIALITY AVAILABILITY
INTEGRITY AUTHENTICITY
NONREPUDIATION

Guarantees the identity of the person, computer or information.

You need to keep an eye out for information that comes from someone who is suspicious, or, if the information seems out of the ordinary, bring it to someone's attention - your supervisor or security officer. Sometimes a seemingly minor detail can turn out to be of the utmost importance.

Lesson 1 - Information Systems Security and IA

Introduction
What's IA?
Foundation for IA
The Future
Goals of IA
Your Role in Security
Summary
Topics

Goals of IA

Glossary Term: Nonrepudiation

The five goals of IA are confidentiality, integrity, availability, authenticity, and nonrepudiation. Click on the green buttons to learn about these goals.

Nonrepudiation

CONFIDENTIALITY AVAILABILITY
INTEGRITY AUTHENTICITY
NONREPUDIATION

Verifies receipt of electronic transactions.

You can help make sure that this is done by tracking sent and received electronic transactions. Your email may offer this as an option.

Lesson 2 - Threats and Vulnerabilities

Introduction
What is a Threat?
Types of Threats
Internal Threats
External Threats
Vulnerabilities
Summary

Topics

Introduction

Glossary Term:
DOD

Threats have become a focus for our society. Most of us have either encountered some threat or we know someone who has encountered a threat. Email viruses and hackers are two types of threats you might encounter while working with the DOD computer systems.

In this lesson, we are going to discuss threats, vulnerabilities, and some myths associated with these threats and vulnerabilities.

Learning Objectives

After you have completed this lesson you will be able to

- Describe some possible threats
- Identify the two types of threats
- Identify the categories of threats
- Give an example of a vulnerability

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 2 - Threats and Vulnerabilities

Introduction
What is a Threat?
Types of Threats
Internal Threats
External Threats
Vulnerabilities
Summary

Topics

What is a Threat?

Glossary Term:
Information System

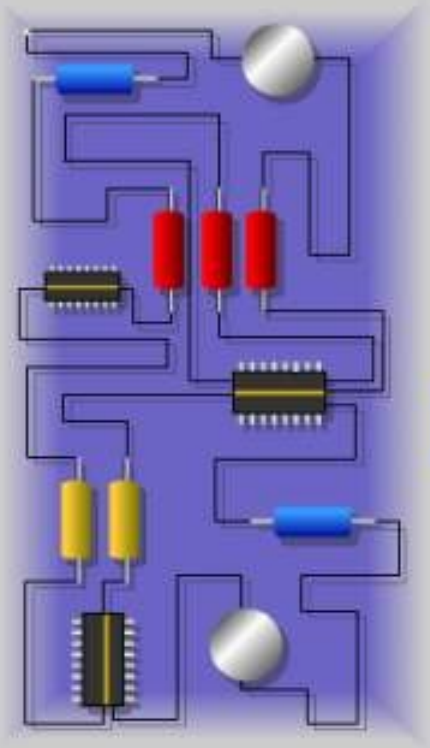
A threat is defined as any circumstance or event with the potential to adversely impact an Information System (IS) through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Lesson 2 - Threats and Vulnerabilities

Introduction
What is a Threat?
Types of Threats
Internal Threats
External Threats
Vulnerabilities
Summary

Types of Threats

Threats are classified into one of two types - internal and external threats.



Internal

External

REPLAY

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 2 - Threats and Vulnerabilities

Internal Intentional and Unintentional Threats

Glossary Term:
Internal Threat

Introduction
What is a Threat?
Types of Threats
Internal Threats
External Threats
Vulnerabilities
Summary

Topics

Internal

Internal threats are threats that originate inside an organization. These threats are further categorized as either intentional or unintentional.

Click the green buttons below to see possible motives and examples of these threats.

Internal Intentional Threats

Internal Unintentional Threats

Lesson 2 - Threats and Vulnerabilities

Introduction
What is a Threat?
Types of Threats
Internal Threats
External Threats
Vulnerabilities
Summary

Topics

Internal Intentional and Unintentional Threats

Glossary Term:
Internal Threat

Internal intentional threats are planned and malicious in nature.

An example of a possible internal intentional threat would be a disgruntled Marine or employee. Because of the potential damage, disgruntled employees or Marines are thought to be the greatest potential threat faced by companies and governments.

Lesson 2 - Threats and Vulnerabilities

Introduction
What is a Threat?
Types of Threats
Internal Threats
External Threats
Vulnerabilities
Summary

Internal Intentional and Unintentional Threats

Glossary Term:
Internal Threat

An example of an internal unintentional threat would be an error made by an employee or a Marine.

An unintentional threat might also include equipment failure, compromising emails or operator malfunction.

Unintentional threats are not planned, but "just happen."

Back

Lesson 2 - Threats and Vulnerabilities

Introduction
What is a Threat?
Types of Threats
Internal Threats
External Threats
Vulnerabilities
Summary

Topics

External Intentional and Unintentional Threats

Glossary Term:
External Threat

External

External threats are threats that originate outside an organization. These threats are also categorized as either intentional or unintentional.

Click the green buttons below to see possible motives and examples of these threats.

External Intentional Threats

External Unintentional Threats

Lesson 2 - Threats and Vulnerabilities

Introduction
What is a Threat?
Types of Threats
Internal Threats
External Threats
Vulnerabilities
Summary

Topics

External Intentional and Unintentional Threats

Glossary Term:
External Threat

An example of an external intentional threat would be a computer hacker that enters your system from outside the organization.
The hacker is the threat that we all hear about on the news. For example, recently three sites of a world famous computer software manufacturer were sabotaged by a computer hacker. Although there was no real damage, the hackers were able to control the site for several minutes.

Lesson 2 - Threats and Vulnerabilities

Introduction
What is a Threat?
Types of Threats
Internal Threats
External Threats
Vulnerabilities
Summary

Topics

External Intentional and Unintentional Threats

Glossary Term:
External Threat

An example of an unintentional external threat would be a natural disaster. These threats are also known as environmental threats.

This threat again involves an unforseen event like an earthquake, a power outage or a hurricane.

Lesson 2 - Threats and Vulnerabilities

Introduction
What is a Threat?
Types of Threats
Internal Threats
External Threats
Vulnerabilities
Summary

Topics

What is a Vulnerability?

Glossary Term:
Vulnerability

A vulnerability is a weakness in an IS, system security procedures, internal controls, or implementation that could be exploited.

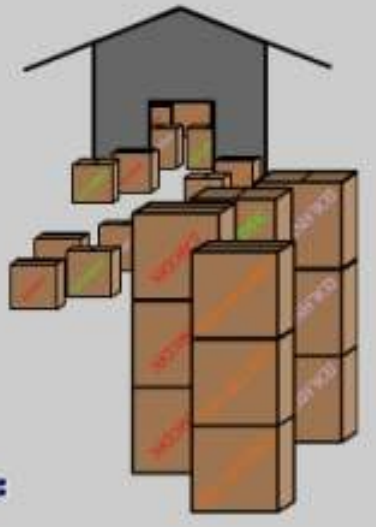
Introduction
What is a Threat?
Types of Threats
Internal Threats
External Threats
Vulnerabilities
Summary

Vulnerabilities (con't)

Vulnerabilities

Some other vulnerabilities that you might see include:

- Audits not maintained/reviewed
- Lack of safeguards
- Lack of maintenance/redundancy
- Infrequent password changes
- Use of group logons



Vulnerabilities can also be found where there are inadequacies (another form of weakness) such as:

- Inadequate training
- Inadequate off-site storage
- Inadequate updates
- Inadequate virus control software

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Common Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary

Topics

Introduction

In this lesson we are going to discuss why you should be concerned with countermeasures, the countermeasures available to you, and who you should call for assistance.

Learning Objectives

After you have completed this lesson you will be able to:

- Identify common countermeasures you can use
- Identify the IA assurance resource person

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Common Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary

Topics

Introduction

In this lesson we are going to discuss why you should be concerned with countermeasures, the countermeasures available to you, and who you should call for assistance.

Learning Objectives

After you have completed this lesson you will be able to:

- Identify common countermeasures you can use
- Identify the IA assurance resource person

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 3 - Countermeasures

Introduction

What is a Countermeasure?

Common Countermeasures

What you can do

Passwords

Who to Call for Assistance

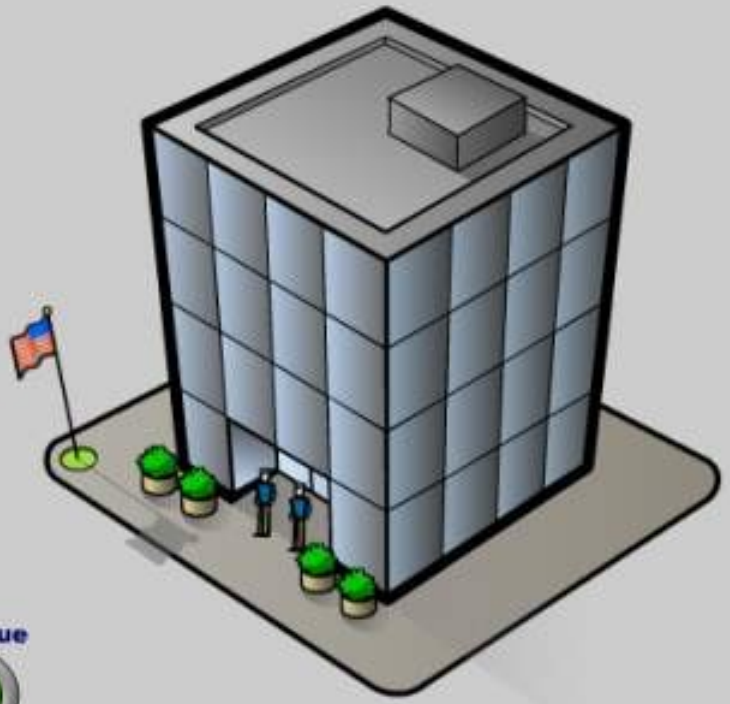
Summary

Topics

Common Countermeasures

Some of the common countermeasures that you might see and use include:

- Tighten physical access



Continue

4 of 16

Main Menu | Course Map | Show Text | Glossary | References | Help | Exit

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 3 - Countermeasures

Introduction

What is a Countermeasure?

Common Countermeasures

What you can do

Passwords

Who to Call for Assistance

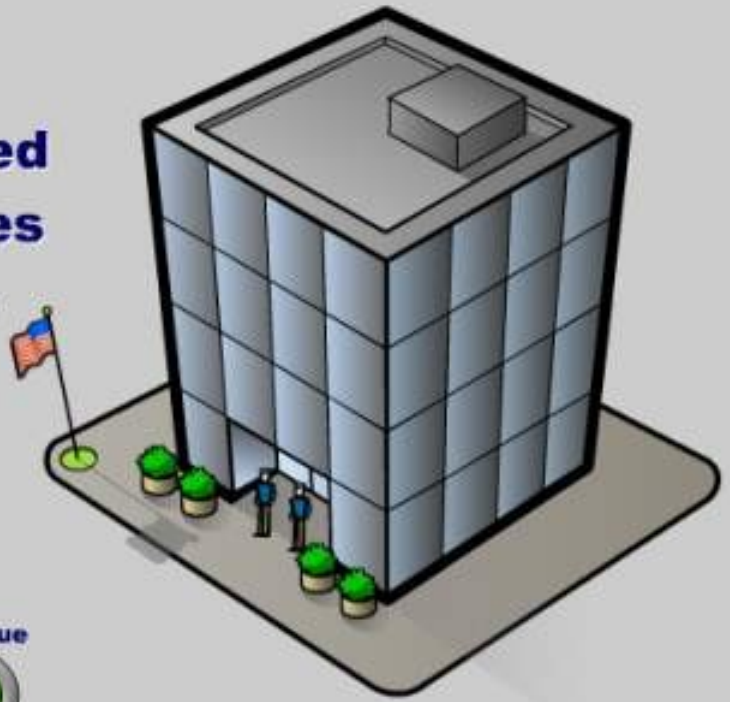
Summary

Topics

Common Countermeasures

Some of the common countermeasures that you might see and use include:

- Deny terminated employees access



Continue

4 of 16

Main Menu | Course Map | Show Text | Glossary | References | Help | Exit

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Common Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary
Topics

Common Countermeasures

Some of the common countermeasures that you might see and use include:

- Force password changes

Continue

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Common Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary
Topics

Common Countermeasures

Some of the common countermeasures that you might see and use include:

- Establish dial-in identification

Continue

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 3 - Countermeasures

Introduction

What is a Countermeasure?

Common Countermeasures

What you can do

Passwords

Who to Call for Assistance

Summary

Topics

Common Countermeasures

Some of the common countermeasures that you might see and use include:

- Security awareness training kept current

Continue

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Common Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary
Topics

Common Countermeasures

Some of the common countermeasures that you might see and use include:

- Increase data/ software backup

MEMO:

As of 05-23-01, we will begin backing up all computers every night rather than the twice a week we have been doing.

Continue

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Common Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary
Topics

Common Countermeasures

Some of the common countermeasures that you might see and use include:

- User agreements

Continue

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Common Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary
Topics

Common Countermeasures

Some of the common countermeasures that you might see and use include:

- Enhanced virus checking

Continue

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Common Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary
Topics

Common Countermeasures

Some of the common countermeasures that you might see and use include:

- Employ a UPS (Uninterruptable Power Supply)

REPLAY

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 3 - Countermeasures

Introduction

What is a Countermeasure?

Examples of Countermeasures

What you can do

Passwords

Who to Call for Assistance

Summary

Topics

What You Can Do

Glossary Term:
System Security Plan (SSP)

You, the end-user, are expected to:

- Know and use proper IA procedures
- Know and employ the System Security Plan (SSP)
- Report all suspected and actual incidents to the Information Systems Security Manager/Officer (ISSM/ISSO)

REPLAY

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Examples of Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary

Topics

Passwords

Glossary Term: Password

A password is a protected/private alphanumeric string used to authenticate an identity or to authorize access to data.

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 3 - Countermeasures

Introduction

What is a Countermeasure?

Examples of Countermeasures

What you can do

Passwords

Who to Call for Assistance

Summary

Topics

Passwords (con't.)

When you choose your password you should:

- **Make your password at least 8 characters long**

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Examples of Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary

Topics

Passwords (con't.)

When you think about choosing your password there are some guidelines you should keep in mind including:

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Examples of Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary

Passwords (con't.)

When you think about choosing your password there are some guidelines you should keep in mind including:

- Not too short, not too long

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Examples of Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary

Topics

Passwords (con't.)

When you think about choosing your password there are some guidelines you should keep in mind including:

- No personal traits

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 3 - Countermeasures

Introduction

What is a Countermeasure?

Examples of Countermeasures

What you can do

Passwords

Who to Call for Assistance

Summary

Topics

Passwords (con't.)

When you think about choosing your password there are some guidelines you should keep in mind including:

- Treat your password like your TOOTHBRUSH:

Use it daily
Change it often
Don't share it with anyone

REPLAY

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Examples of Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary
Topics

Passwords (con't.)

If you are still unsure of what good and bad passwords include, there are examples of both listed below.

If you are still unsure of what good and bad passwords include, here are examples of both:

GOOD PASSWORDS	BAD PASSWORDS
- p3yUhd0G	- mykittycat
- 9Lkw3G8u	- hypochondriac
- u1hta89S	- computer
- Q2o0dDj4	- maryanne

REPLAY

Introduction
What is a Countermeasure?
Examples of Countermeasures
What you can do
Passwords
Who to Call for Assistance
Summary

Topics

Who to Call for Assistance

Glossary Term:
System Security Officer/ Manager (ISSO/ISSM)

Having a problem? Who do you call?

Lesson 3 - Countermeasures

Who to Call for Assistance (con't)

Glossary Term:
INFOSEC

The ISSO oversees and is responsible for:

- Encouraging responsible use
- Making users aware of policies
- Enforcing policies

Click "Continue" for other responsibilities

Continue

Introduction
What is a Countermeasure?
Examples
Who to Call for Assistance
Passwords
Summary

Topics

Lesson 3 - Countermeasures

Introduction

What is a Countermeasure?

Examples of Countermeasures

What you can do

Passwords

Who to Call for Assistance

Summary

Topics

Who to Call for Assistance (con't)

Glossary Term:
INFOSEC

The ISSO oversees and is responsible for:

- Unit IA awareness training

Continue

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Examples
What you can do
Passwords
Who to Call for Assistance
Summary

Topics

Who to Call for Assistance (con't)

Glossary Term:
INFOSEC

The ISSO oversees and is responsible for:

- **Unit IA readiness evaluation**

Continue

Lesson 3 - Countermeasures

Introduction
What is a Countermeasure?
Examples
What you can do
Passwords
Who to call for assistance
Summary

Topics

Summary

In this lesson we covered the definition of a countermeasure and some common countermeasures you will probably see and use when working on the DOD's computer system. We also discussed who you should contact when there is a problem or when you have a question. In the next lesson we are going to talk about Software Security.

Click the forward button to return to the Lesson Menu

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Introduction

In this lesson we are going to cover Software Security, handling and destroying classified and unclassified information, malicious software, viruses, and network security and controls.

Learning Objectives

After you have completed this lesson you will be able to:

- Identify the differences between classified and unclassified information
- Identify the procedures used to handle unclassified but sensitive, and classified information
- Determine the best method to be used to destroy data
- Identify some forms of malicious software
- Define the term Firewall

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

What is Software Security?

IRM 5239-08

SOFTWARE SECURITY:

"General purpose (executive, utility, or software development tools) and application programs or routines that protect data handled by a system."

Some examples of this include:

- Your operating system
- Your applications
- Your data files

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Classified and Unclassified Information

Glossary Terms:
Classified Data/Information
Unclassified Data/Information

Data is classified by the originator into one of two categories

Classified - which includes data that is considered Confidential, Secret and Top Secret.

Unclassified - which includes sensitive data that falls under the Privacy Act or is considered to be Privileged, Proprietary or For Official Use Only (FOUO).

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Classified and Unclassified Information (con't)

Sensitive unclassified information must be processed and stored on separate, dedicated information systems independent of those used for classified information.

SERVER - SENSITIVE INFORMATION
SERVER - CLASSIFIED INFORMATION
No Data Interchange between Classified systems and Sensitive systems
WARNING: Never put classified information on an unclassified system!
SENSITIVE
CLASSIFIED
REPLAY

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 4 - Software Security

Introduction

What is Software Security?

Classified and Unclassified Information

Malicious Software

Viruses

Network Security

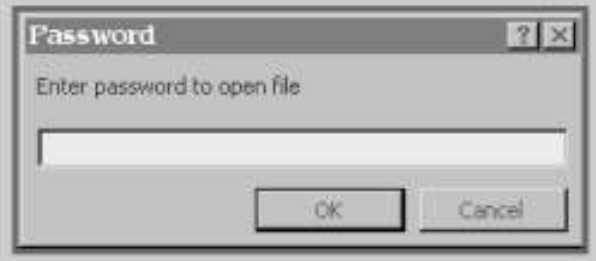
Summary

Topics

Classified and Unclassified Information (con't)

When handling unclassified information you need to:

- **Place proper account controls on all system accounts**



Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Classified and Unclassified Information (con't)

When handling unclassified information you need to:

- **Ensure only authorized personnel have access to the information**

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Classified and Unclassified Information (con't)

When handling unclassified information you need to:

Continue

- Ensure that only the people with a need to know have access to information

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Classified and Unclassified Information (con't)

When handling unclassified information you need to:

- **Correctly dispose of materials containing this information**

Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Classified and Unclassified Information (con't)

When handling unclassified information you need to:

- Store backup copies in a secure, off-site location

REPLAY

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Classified and Unclassified Information (con't)

All information and information systems must be labeled and marked correctly using the following system

- Unclassified SF 710 (Green)

- Classified SF 709 (Purple)

- Top Secret SF 706 (Orange)

- Secret SF 707 (Red)

- Confidential SF 708 (Blue)

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Classified and Unclassified Information (con't)

Glossary Term: GSA

What do you do with the information once you are through working with it?

Classified information needs to be stored in a GSA-approved container in an area cleared for storage of classified information.

Sensitive unclassified information should be stored in a locked drawer or a container that has more security than an unsecure drawer.

Finally, store a copy of backups in a secure off-site location.

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Classified and Unclassified Information (con't)

Glossary Term:
Degaussing

The destruction of information may also require additional planning.

For example, to destroy unclassified information, the Department of the Navy (DoN) will allow you to use "wipedisk" or "wipefile". Degaussing, shredding, and burning are not required.

Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Classified and Unclassified Information (con't)

Glossary Term:
Degaussing

The destruction of information may also require additional planning.

However, if you are destroying classified information you must have the correct documentation. Without this documentation the information is considered lost and needless fear of a security breach may be suspected, investigated, and you may be held accountable for the loss.

Lesson 4 - Software Security

Introduction
What is Software Security?
Objectives and Importance of Information Assurance
Malicious Software
Viruses
Network Security
Summary
Topics

Malicious Software

Malicious software is any software designed to cause damage to, or use up the resources of, a computer.

It is frequently part of or disguised as authentic software. Sometimes it infects other computers through email or contaminated floppy disks.

REPLAY

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Malicious Software (con't)

Types of malicious software include viruses, Trojan Horses, worms, and bombs. To find out more about these forms of malicious software click on the pictures or buttons as appropriate.

Trojan Horse

Virus

Worm

Bomb

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Viruses

Viruses can spread in numerous ways. The most common ways include using:

- Floppy diskettes brought in by employees from outside the facility

Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Viruses

Viruses can spread in numerous ways. The most common ways include using:

- Shrink-wrapped software

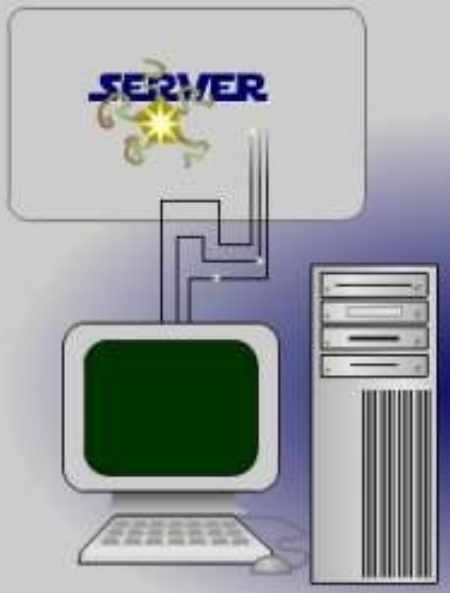
Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Viruses

Viruses can spread in numerous ways. The most common ways include using:



- Networks that have been infected at workstations

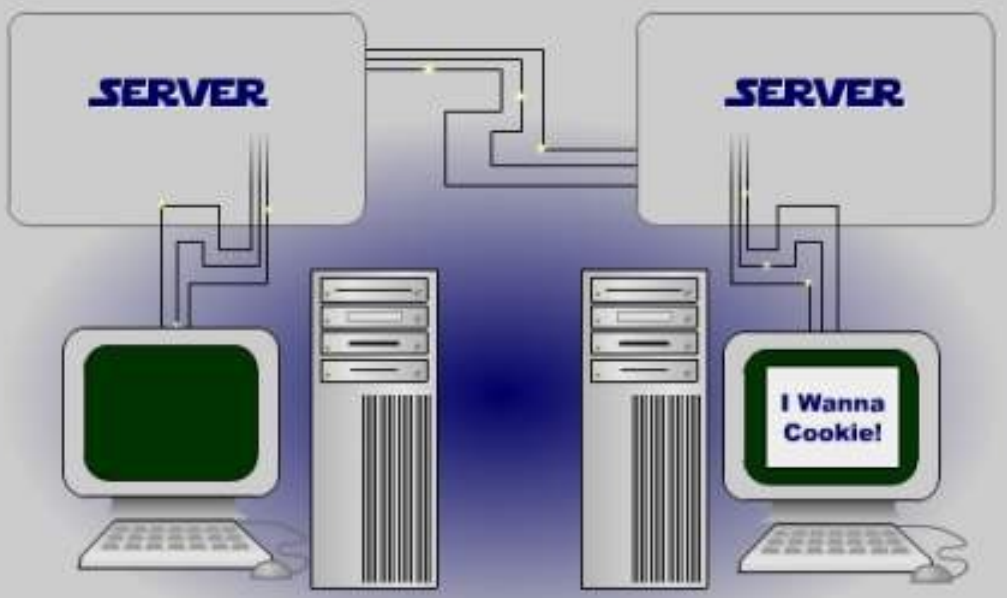
Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary
Topics

Viruses

Viruses can spread in numerous ways. The most common ways include using:



- Email between home and office

To see how a virus is usually spread, click "Continue"

Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Viruses (con't)

Viral symptoms can take many forms. Some of the more common symptoms that you might notice include:

- Your program suddenly takes longer to load
- Your program size keeps changing
- Your disk keeps running out of free space
- You have files on your system but you do not know where they came from
- Your files have strange names
- An animation you did not load will move across your screen

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Viruses (con't)

Viral symptoms can take many forms. Some of the more common symptoms that you might notice include:

- Your program suddenly takes longer to load
- Your program size keeps changing
- Your disk keeps running out of free space
- You have files on your system but you do not know where they came from
- Your files have strange names
- An animation you did not load will move across your screen

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Viruses (con't)

Glossary Term:
BBS

Some of the common myths believed by most users include:

- **Viruses destroy hardware**
- **Assigning a READ-ONLY attribute will prevent infection**
- **Viruses infect write-protected diskettes**
- **BBS/shareware are the primary sources**
- **Backups are useless**

These myths are untrue!
Do not believe them!

Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Viruses (con't)

Glossary Term:
BBS

Some of the common myths believed by most users include:

- **Viruses destroy hardware**
- **Assigning a READ-ONLY attribute will prevent infection**
- **Viruses infect write-protected diskettes**
- **BBS/shareware are the primary sources**
- **Backups are useless**

These myths are untrue!
Do not believe them!

Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Viruses (con't)

When you discover a virus, you need to immediately:

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Viruses (con't)

When you discover a virus, you need to immediately:

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Viruses (con't)

When you discover a virus, you need to immediately:

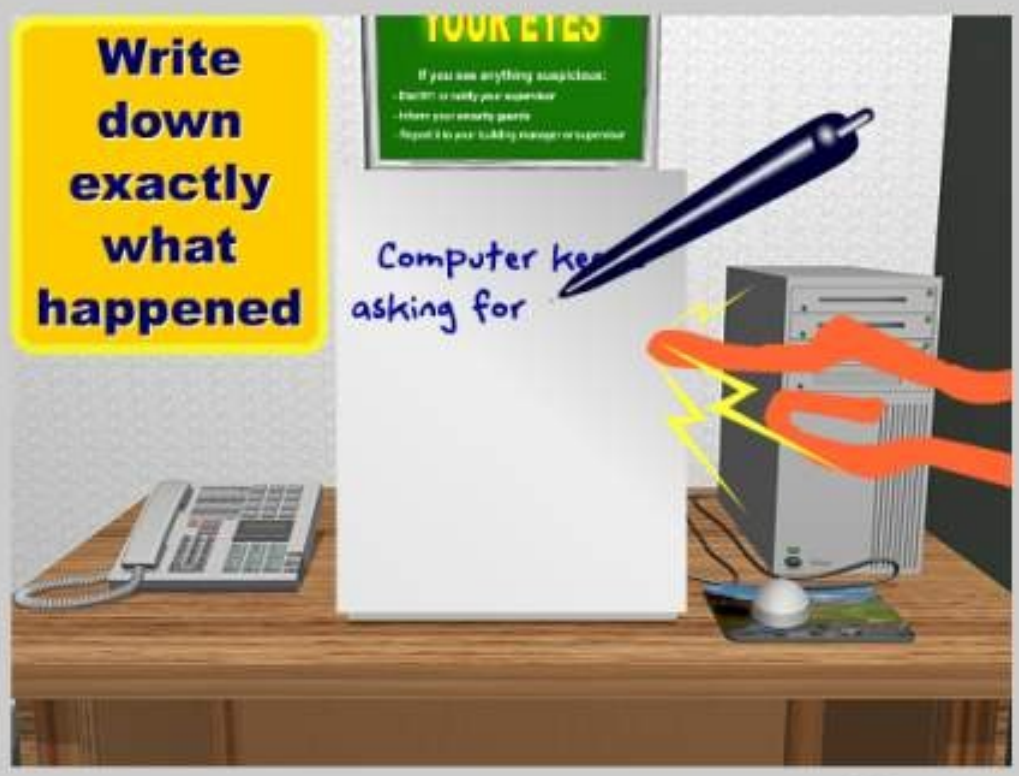
Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Viruses (con't)

When you discover a virus, you need to immediately:



Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Viruses (con't)

When you discover a virus, you need to immediately:

WARNING:

DO NOT

DELETE

the infected file!

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Viruses (con't)

When you discover a virus, you need to immediately:

DO NOT

PANIC

Viruses will not hurt your equipment.

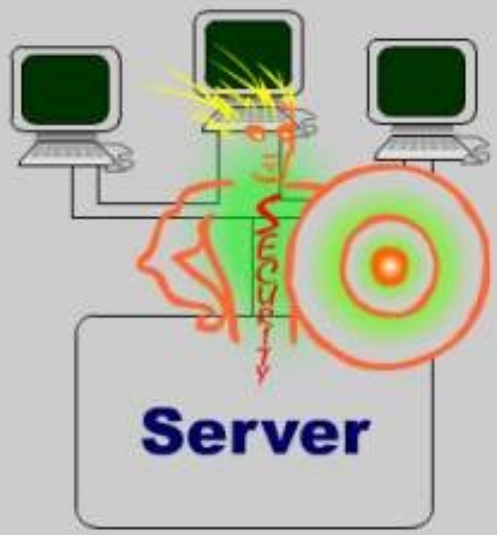
REPLAY

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Network Security



Network Security includes the mechanisms and procedures in place to protect network assets.

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Network Security

Network Security includes the following controls:

Locking and logging off your computer

- Terminal Security

Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Network Security

Network Security includes the following controls:

Passwords and User Names - **Identification and Authentification**

Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Network Security

Network Security includes the following controls:

Blocking access after three tries

- Limited Logon attempts

Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Network Security

Network Security includes the following controls:

Ending inactive Sessions

- Automatic termination

Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Network Security

Network Security includes the following controls:

Allowing only certain data types in and out

- Firewalls

Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Network Security

Network Security includes the following controls:

Maintaining a log of all activity

- Audit trails

REPLAY

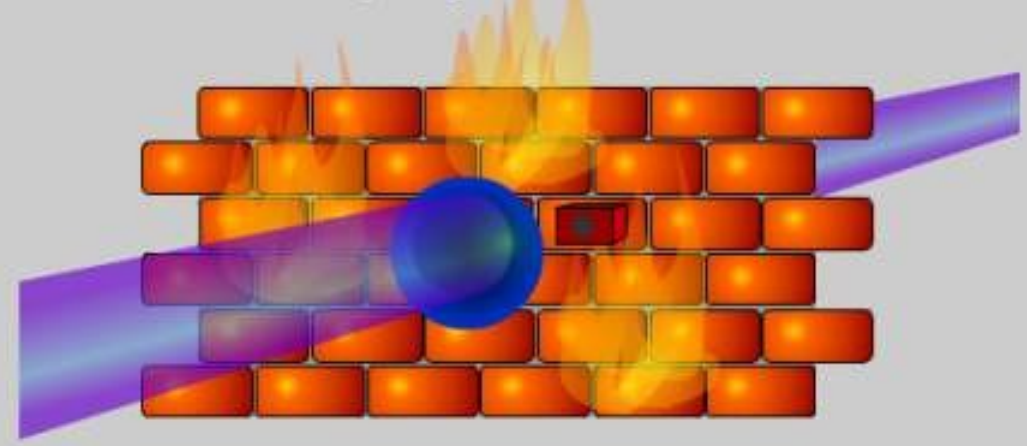
Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Network Security (con't)

Firewalls are one piece of network security.

A firewall is a system or group of systems that enforce an access control policy between two networks.



In other words, a firewall is a security system used to protect computers from damage or unauthorized access.

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Network Security (con't)

You play a role in how well the network security functions. In order for the network security to function at an optimal level, you need to:

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Network Security (con't)

You play a role in how well the network security functions. In order for the network security to function at an optimal level, you need to:

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Network Security (con't)

You play a role in how well the network security functions. In order for the network security to function at an optimal level, you need to:

- Limit visitor access to terminal area and system
MEMO:
No one is to be allowed in any room with computers without a pass.
Report any person who does not seem to belong or has no pass.
Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Network Security (con't)

You play a role in how well the network security functions. In order for the network security to function at an optimal level, you need to:

- Activate "terminal timeout" options
This terminal has been idle for 30 minutes. It will shut down in 2 minutes if there is no activity in that time.
Continue

Lesson 4 - Software Security

Introduction
What is Software Security?
Classified and Unclassified Information
Malicious Software
Viruses
Network Security
Summary

Topics

Network Security (con't)

You play a role in how well the network security functions. In order for the network security to function at an optimal level, you need to:

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Countermeasures The SSP
Your Role
Your Equipment
Summary

Topics

Introduction

In this lesson we are going to cover physical security and hardware security. We are also going to look at areas of concern in relation to physical security; your role and responsibilities as an end-user; and the countermeasures that are used with physical security.

Learning Objectives

After you have completed this lesson you will be able to:

- Identify the concerns of hardware security
- Identify the environmental threats and areas of concern regarding physical security
- Identify the end-users' roles and responsibilities regarding physical security
- Describe the countermeasures used with physical security

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Countermeasures The SSP
Your Role
Your Equipment
Summary

Topics

What is Physical Security?

According to the National Security Telecommunications and Information Systems Security Committee (NSTISSC) physical security is:

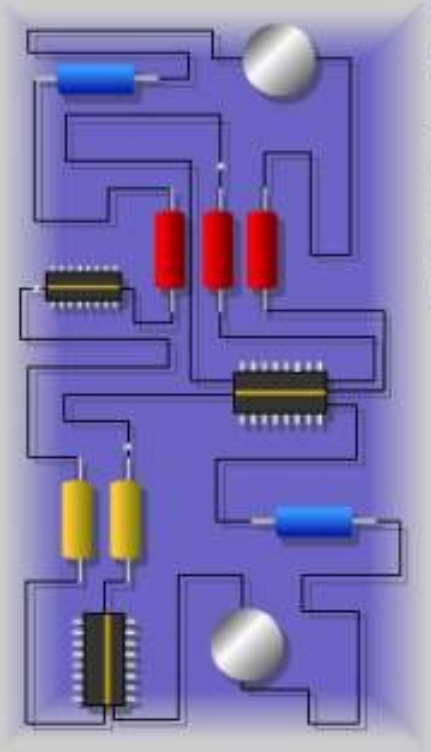
"...the protection and preservation of informational, physical, and human assets by reducing exposure to various threats which can produce a disruption or denial of AIS (Automated Information System) services or unauthorized disclosure or access to those assets."

In other words, physical security should cause the number of threats that frequently cause the problems mentioned above to become much smaller.

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Countermeasures The SSP
Your Role
Your Equipment
Summary
Topics

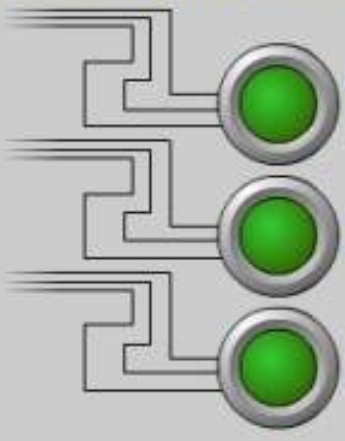
Threats to Physical Security



The basic threats to physical security include:

- **Intentional Acts**
- **Unintentional Acts (human error)**
- **Natural Disasters**

To get more information about these threats, click the green buttons below.



Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Countermeasures The SSP
Your Role
Your Equipment
Summary
Topics

Threats to Physical Security

Intentional acts are planned and usually malicious.

Intentional acts might include:

- **Casual intruders**
- **Disgruntled employee/Marine**
- **Skilled intruder**
- **Vandalism**
- **Sabotage**
- **Terrorism**
- **Virus producer**

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Countermeasures
The SSP
Your Role
Your Equipment
Summary
Topics

Threats to Physical Security

Unintentional threats are the product of human error. This is something you can be aware of but may not be able to prevent. Usually unintentional threats are less severe than the other types of threats encountered in physical security.

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Countermeasures The SSP
Your Role
Your Equipment
Summary
Topics

Threats to Physical Security

Natural disasters, such as hurricanes and earthquakes, are uncontrollable and can cause extensive damage to computer systems.

Countermeasures for these threats require using contingency plans and awareness training.

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Countermeasures The SSP
Your Role
Your Equipment
Summary
Topics

Hardware Security

Hardware security is concerned with the protection and control of electric, electronic and mechanical equipment used for processing data.

When talking about hardware security, there are several areas of particular concern. These areas include:

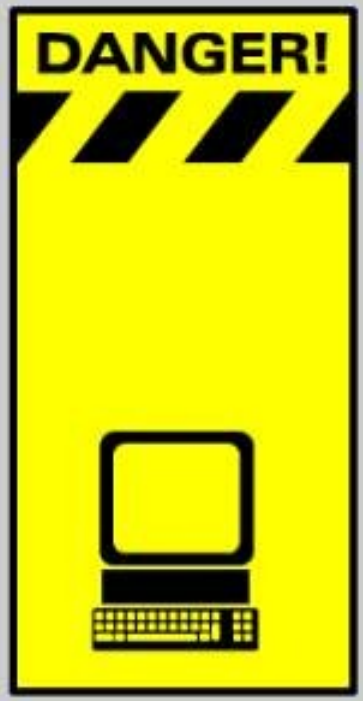
- **System access**
- **Smoking, eating or drinking near computers**
- **Disk handling**
- **System modifications**
- **Theft**

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Environmental Concerns/Threats
Countermeasures The SSP
Your Role
Your Equipment
Summary
Topics

Environmental Concerns/Threats

Most computers are created to function in an office environment where climate and other factors are controlled. However, there are still threats and areas of concern that include:



- Fire
- Water Damage
- Excessive Heat
- Power Surges (static electricity)
- Airborne Contaminants

REPLAY

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 5 - Physical Security

Introduction

What is Physical Security?

Threats to Physical Security

Hardware Security

Environmental Concerns/Threats

Countermeasures The SSP

Your Role

Your Equipment

Summary

Topics

Countermeasures - The SSP

Glossary Term:
Contingency Plan

The main countermeasures for Physical Security is you, the end user, and a GOOD System Security Plan (SSP). A good SSP considers the environment, the files and contingency plans. Click on the green buttons below to learn more about these factors.

- Environment
- Files
- Contingency Plan

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Countermeasures The SSP
Your Role
Your Equipment
Summary
Topics

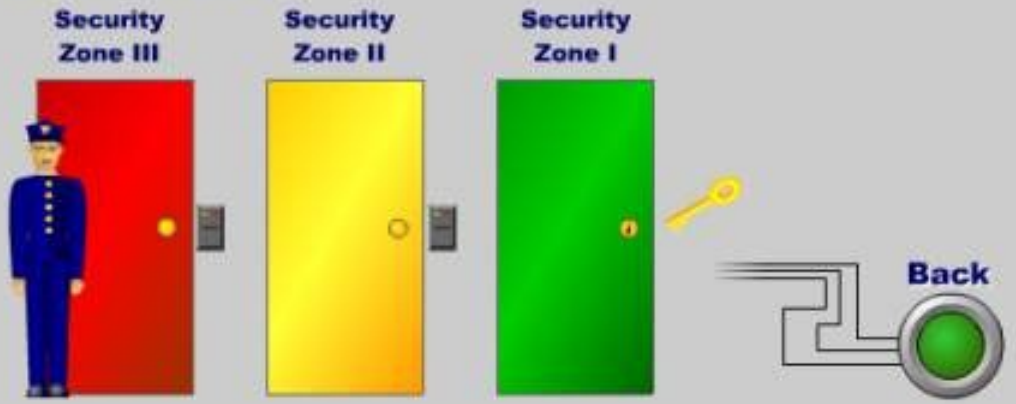
Countermeasures - The SSP

Glossary Term:
Contingency Plan

A good SSP will look at how your environment is secured. This level of security is determined by the type, and the sensitivity of information your unit creates, processes, stores or destroys.

These factors also establish the level of access for your environment.

There are three levels of Security Zones which include a variety of security measures prescribed by MCO P5510.14.



Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Countermeasures
The SSP
Your Role
Your Equipment
Summary
Topics

Countermeasures - The SSP

Glossary Term:
Contingency Plan

A good SSP considers the accessibility of your files, both electronic and paper-based.

The SSP should provide controlled access to your files.

Back

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Countermeasures
The SSP
Your Role
Your Equipment
Summary
Topics

Countermeasures - The SSP

Glossary Term:
Contingency Plan

A good SSP makes use of contingency plans to minimize the effects of disasters.

Back

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 5 - Physical Security

Introduction

What is Physical Security?

Threats to Physical Security

Hardware Security

Environmental Concerns/Threats

Protecting Yourself on the SIPR

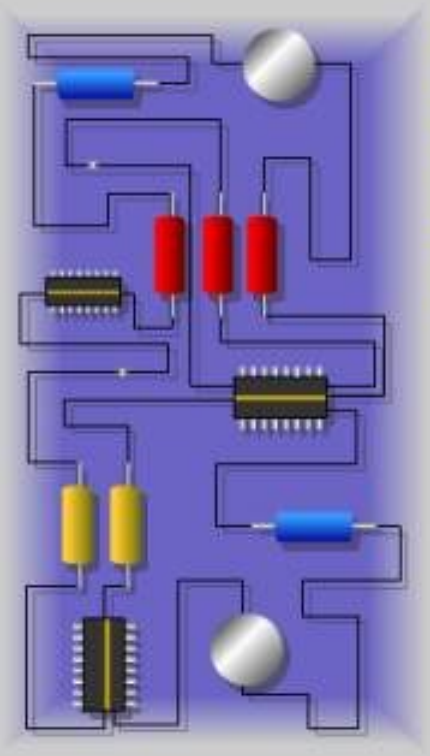
Your Role

Your Equipment

Summary

Topics

Your Role



As a member of the active military or the civilian workforce, you have certain responsibilities to protect your workplace. There are several things you can do to keep your work and workplace secure. Click the green buttons below to see how you can help maintain physical security.

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Workforce Security
Environmental Concerns/Threats
Protecting Yourself and the DSP
Your Role
Your Equipment
Summary
Topics

Your Role

You can keep an eye on your surroundings. Is someone going into files that are restricted? Are there strangers in your area? Are the doors to restricted access shut and locked?

Back

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Contingency Planning and the SSP
Your Role
Your Equipment
Summary
Topics

Your Role

When you leave your computer, make sure that you log out or lock the system. Leaving someone access to an open computer may cause a serious breach in security.

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 5 - Physical Security

Introduction

What is Physical Security?

Threats to Physical Security

Maintaining Security

Environmental Concerns/Threats

Contributions of the ISSP

Your Role

Your Equipment

Summary

Topics

Your Role

You can be aware of your surroundings and day-to-day routine. Small changes that go unnoticed by many may be significant indicators of security issues.

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Controlling Access to the ISSP
Your Role
Your Equipment
Summary

Topics

Your Role (con't.)

You are responsible not only for your work area, but also for the security of your workstation.

To ensure that your workstation is secure you need to:

- **Lock your workstation whenever you leave the immediate area**

Continue

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
Hardware Security
Environmental Concerns/Threats
Contingency Planning for the ISSP
Your Role
Your Equipment
Summary

Topics

Your Role (con't.)

You are responsible for the security of your workstation. To ensure that your workstation is secure you need to:

- **LOG OFF** when you are leaving for a significant period of time

Continue

Information Assurance (IA) / Awareness [WEB] - Microsoft Internet Explorer provided by NMCI

Lesson 5 - Physical Security

Your Role (con't.)

Do your part!!!

Secure your workstation!

REPLAY

Introduction

What is Physical Security?

Threats to Physical Security

Hardware Security

Environmental Concerns/Threats

Contingency Planning and the ISSP

Your Role

Your Equipment

Summary

Topics

8 of 15

Main Menu | Course Map | Show Text | Glossary | References | Help | Exit

Lesson 5 - Physical Security

Introduction
What is Physical Security?
Threats to Physical Security
U.S. Force Protection
Environmental Concerns/Threats
Contingency Issues in the AOR
Your Role
Your Equipment
Summary
Topics

Your Equipment

Glossary Terms:
PED MCEN
PDA FIPS

Using PEDs (Personal Electronic Devices) is a popular and functional way to assist you with your work. PEDs also present another risk factor that must be considered.

The Marine Corps is developing a policy to counter the risks associated with PEDs. Some of the major provisions in the policy include:

- PEDs with RF/Wireless capabilities are **not** authorized in classified workspaces.
- PEDs will only be connected to unclassified government computers at locations designated and approved by an authorized DAA (Designated Approving Authority).
- Only government owned and issued PEDs are authorized to connect to the MCEN (Marine Corps Electornic Network)..
- Only government PED versions that have FIPS 140-1 validation can establish wireless connections to the MCEN.
- PED modems cannot be used while connected to a network computer.
- Government owned PEDs cannot be connected to personally owned computer equipment.